BlackBerry Smartphone

Version: 7.1

Security Feature Overview

Published: 2012-10-30
SWD-20121030142958167

Contents

Overview 4

Security features 5
Browsing and connecting to the Internet 5
BlackBerry ID 5
BlackBerry Bridge app 5
Protecting Wi-Fi connections 6
Spam email messages 6
Attachments 6
BlackBerry Smart Card Reader 7

Security options 8
Using a smartphone password 8
Controlling downloaded applications 8
Protecting your GPS location information 9
Protecting NFC connections 9
Protecting Bluetooth connections 10
Protecting passwords that your smartphone stores 10
Encrypting your smartphone data 10
Encrypting files that are stored on a media card 11
Blocking messages 11
Cleaning memory 11
Deleting all BlackBerry smartphone data 12

Find more information 13

Legal notice 14

Overview

Your BlackBerry smartphone is designed to help protect your data, personal information, and storage spaces from unauthorized access. Your smartphone is designed to provide secure connections to the wireless network and to other devices.

You can change options on your smartphone, such as setting a password and turning on encryption for your data and files, to help protect your smartphone from unauthorized access and use.

Security features

Browsing and connecting to the Internet

Your BlackBerry smartphone creates an encrypted connection to banking websites and shopping websites that support encryption, such as the BlackBerry App World storefront. Using an encrypted connection, especially during online banking transactions, ecommerce transactions, and other wireless transactions on mobile devices and computers, helps to protect you against identity theft and unauthorized use of your financial data.

You can determine whether encryption is helping to protect data that you send or receive using the BlackBerry Browser. When you are using an encrypted connection, a lock icon appears on the right side of the address bar on the browser screen.

BlackBerry ID

A BlackBerry ID is a single sign-on identity service that gives you convenient access to multiple BlackBerry products, sites, services, and apps. After you create a BlackBerry ID, you can use a single email address and password to log in to any BlackBerry product that supports BlackBerry ID.

A BlackBerry ID is designed to protect your account information from unauthorized access. When you create or log in to your BlackBerry ID, encryption helps protect your information.

BlackBerry Bridge app

Your BlackBerry PlayBook tablet is designed to open an encrypted and authenticated connection to your BlackBerry smartphone by using the BlackBerry Bridge app and Bluetooth technology.

If your tablet connects to a smartphone that is associated with the BlackBerry Internet Service only, then the data that the smartphone stores on the tablet is considered personal data. Personal data that is stored on the tablet isn't encrypted.

If your tablet connects to a smartphone that is associated with a BlackBerry Enterprise Server, when you use the BlackBerry Bridge app to connect your tablet to a smartphone, the data that the smartphone stores on the tablet is isolated as BlackBerry Bridge data. BlackBerry Bridge data is stored separately from the personal data and work data on your tablet. BlackBerry Bridge data is encrypted and stored on the tablet temporarily. When you close the connection between your tablet and from your smartphone, the BlackBerry Bridge data is no longer accessible on your tablet. Your personal data and apps remain intact.

If you set a password for your smartphone, you must provide the smartphone password when your tablet accesses any smartphone data. Your smartphone password settings, such as the security timeout setting, are extended to the tablet. For example, if you set your smartphone to lock after five minutes of inactivity and you don't use the BlackBerry Bridge app for five minutes, you might be prompted to enter your smartphone password when you use the BlackBerry Bridge app again.

For more information about BlackBerry Bridge security features, visit www.blackberry.com/go/serverdocs and click Security > BlackBerry PlayBook Security.

Protecting Wi-Fi connections

If supported by your wireless service provider, a Wi-Fi enabled BlackBerry smartphone can access the BlackBerry Infrastructure using a reliable and secure transport when using Wi-Fi connections.

To help protect the communication throughout the unprotected networks, your smartphone supports negotiating encrypted connections to the BlackBerry Infrastructure to establish a browsing connection to the Internet using a Wi-Fi connection.

Your smartphone can also support multiple security methods that are designed to encrypt wireless communications over the Wi-Fi network between the smartphone and either the wireless access points or a network firewall. Your smartphone is designed to reject incoming connections, to support limited connections in Wi-Fi infrastructure mode only, and to prevent Wi-Fi peer-to-peer (ad-hoc networking) connections.

For more information about Wi-Fi enabled BlackBerry smartphones, visit http://na.blackberry.com/eng/ataglance/networks/#tab_ddetail_subtab_wifi.

Spam email messages

If your BlackBerry smartphone is associated with the BlackBerry Internet Service, your smartphone uses an antispam system that is designed to block spam email messages that are sent to your BlackBerry email address. This feature helps to protect you against the inconvenience and potential privacy threat of receiving email messages that are not intended for you.

For additional control of spam email messages, you can create email message filters to prevent unwanted email messages from being delivered to your smartphone.

Attachments

Your BlackBerry smartphone doesn't run applications that you receive as attachments to email messages. Your smartphone processes attachments and renders them in a format that is designed to protect you from potentially damaging attachment code, such as macros.

To protect the attachments that your BlackBerry smartphone stores, you can turn on encryption.

BlackBerry Smart Card Reader

The BlackBerry Smart Card Reader is an accessory that, when used in proximity to a Bluetooth enabled BlackBerry smartphone or a Bluetooth enabled computer, permits you to authenticate with a smart card and log in to the BlackBerry smartphone or computer.

The BlackBerry Smart Card Reader permits you to prove your identity to your BlackBerry smartphone or computer using what you have (smart card) and what you know (smart card password).

For more information, visit www.blackberry.com/go/serverdocs and see the *BlackBerry Smart Card Reader Security Technical Overview*.

Security options

Using a smartphone password

You can set a password to help protect your BlackBerry smartphone from unauthorized use.

You can also set your smartphone to lock automatically at specified time intervals (for example, every 30 minutes), or to lock when it is inserted in a holster. By default, when you type your smartphone password incorrectly more than 10 times, your smartphone is designed to permanently delete your stored data and application data. You can change how many password attempts are allowed before all data on your smartphone is deleted.

If your smartphone is associated with a BlackBerry Enterprise Server that supports this feature, you can indicate that you are unlocking your smartphone against your will by moving the first character of your password to the end of your password. For example, if your smartphone password is blackberry, to send an email notification that you are under duress you would type lackberryb.

Controlling downloaded applications

Your BlackBerry smartphone includes virus protection and spyware protection that is designed to contain and prevent the spread of viruses and spyware to other applications.

You can download third-party applications for your BlackBerry smartphone over the wireless network from the BlackBerry App World storefront or a website. A third-party application can communicate and share data with other third-party applications and smartphone applications. You can proactively protect your smartphone from viruses and spyware by only downloading applications from trustworthy sources.

When you download an application, you might be prompted to trust the application or to set permissions for it. If you trust the application, your smartphone sets most permissions for the application to Allow. You can change the permissions for a specific application or all applications to control access to the following resources:

Resource	Description
Advanced Capabilties	Set whether third-party applications can perform advanced operations, such as simulating key presses, managing your applications, or modifying Internet browsing.
Appearance Settings	Set whether third-party applications can change settings that affect the visual appearance or behavior of your smartphone, such as preventing your smartphone from locking when it is left idle.
Connectivity	Set whether third-party applications can make phone calls, send text messages, access the Internet, and use other connectivity features. Some applications may send information to third-party companies or create connections that are billable by your wireless service provider.

Resource	Description
Location	Set whether third-party applications can request your smartphone's GPS location. Some applications might share this information with third-party companies or use it for targeted advertising.
Personal Information	Set whether third-party applications can access content, such as your email address, contact information, audio files, video files, and other saved files. Some applications might share your personal information with third-party companies.
Secure Element	Set whether third-party applications can access confidential information that are stored on your smartphone's secure element, such as credit card numbers, coupons, loyalty cards, and public transit passes. Depending on your smartphone model and wireless service provider, your smartphone might not use a secure element.

Protecting your GPS location information

Your BlackBerry smartphone has location security and controls built into it. Websites, third-party applications, and preloaded smartphone applications that support location-based services can potentially track your location or report your location to a server.

In the smartphone options, you can manage access for each application and control exactly which third-party applications have permission to request your smartphone's location. To prevent third-party websites or applications from using the GPS location of your smartphone, you can block third-party applications from using the GPS location information and, in the browser options, you can turn off the geolocation option for sharing your location with websites.

Protecting NFC connections

NFC technology is a short-range, wireless technology that is designed to allow you to quickly exchange information between an NFC-enabled BlackBerry smartphone and NFC-enabled smartphones, smart accessories, NFC-enabled payment terminals, NFC-enabled access points, and smart tags.

An NFC-enabled smartphone uses a secure element to store confidential information, such as credit card numbers, coupons, loyalty cards, and public transit passes. Depending on your smartphone model and wireless service provider, a secure element can be embedded on your smartphone or on a SIM card.

An application can access your smartphone's secure element if you trust the application, or your smartphone is associated with a BlackBerry Enterprise Server. Otherwise, if an application needs to access your smartphone's secure element you are prompted to allow access. You can change your application permissions to always allow, always deny, or require a prompt to access the secure element.

An NFC-enabled BlackBerry smartphone includes the following security measures:

- You can turn off NFC technology on your smartphone.
- By default, your smartphone prompts you each time it tries to send or receive a file using BlackBerry Tag.
- You must request a connection with a smart accessory (for example, by tapping your smartphone on a smart tag).

- You can disable NFC payment transactions when your smartphone is turned off, locked, or the backlight is turned off.

Protecting Bluetooth connections

Using Bluetooth wireless technology, you can open wireless connections between a Bluetooth enabled BlackBerry smartphone and other Bluetooth devices that are within a 10 m range (for example, a hands-free car kit or wireless headset).

Your smartphone creates a Bluetooth profile, which specifies how applications on your smartphone and on other Bluetooth devices connect and communicate.

Your smartphone includes the following security measures:

- You can turn off the Bluetooth wireless technology for your smartphone.
- You can specify whether to encrypt data sent to and from your smartphone over a Bluetooth connection.
- You must request a pairing with another Bluetooth device. You might also need to use a passkey to complete the pairing.
- Your smartphone prompts you each time a Bluetooth device tries to connect to your smartphone.

Protecting passwords that your smartphone stores

You can use the Password Keeper to store all your passwords in one place. The Password Keeper is designed to protect your passwords using a Password Keeper password. You only need to remember the Password Keeper password.

The first time you open the Password Keeper on your smartphone, you must create the Password Keeper password. The Password Keeper is designed to encrypt the information that is stored within it and when you type the Password Keeper password, the Password Keeper decrypts this information. If the number of allowed password attempts in the Password Keeper is exceeded, the Password Keeper data can't be accessed unless your smartphone data is restored and the password used to encrypt the password keeper data is entered.

In the Password Keeper, you can do the following:

- Type a password and its identifying information (for example, which application you can access using the password).
- Generate random passwords that are designed to improve password strength.
- Copy passwords and paste them into an application or password prompt for a website.

Encrypting your smartphone data

Your BlackBerry smartphone is designed to use encryption, with symmetric and asymmetric encryption algorithms and encryption keys, to protect your stored data.

When you turn on encryption in the security options, your smartphone encrypts data stored on your smartphone (for example, browser information, messages, tasks, and calendar entries), including data that your smartphone receives when it's locked. When you lock your smartphone with a password and your smartphone has secured your data, a closed lock indicator appears in the upper-left corner of the screen. If potentially malicious users attempt to access your data directly from the internal smartphone hardware, they can't decrypt and read the data without knowing your smartphone password.

You can set the encryption strength level to optimize either the encryption strength or the decryption time. More encryption strength means a longer decryption process. To maximize encryption strength, it is generally recommended that you increase the length of your smartphone password. If you set the encryption strength to "Stronger", use a minimum length of 12 characters for the smartphone password. If you set the encryption strength to "Strongest", use a minimum length of 21 characters for the smartphone password.

Encrypting files that are stored on a media card

Your BlackBerry smartphone is designed to encrypt media files that you store on a media card using your smartphone password, an encryption key that your smartphone generates, or both.

If you turn on the Encrypt Media Files option and transfer files to your media card using the BlackBerry Desktop Software, Bluetooth technology, or NFC technology, the files can be encrypted and decrypted. If you manually transfer files to or from your media card (for example, to a computer using USB mass storage mode), the files aren't encrypted or decrypted even if you have turned on the Encrypt Media Files option.

For more information about encrypting media card files, visit www.blackberry.com/btsc to read article KB16088.

Blocking messages

You can set up the built-in firewall on your BlackBerry smartphone to block unwanted messages, such as incoming text messages or email messages. If you are blocking messages, you can make exceptions so that your contacts, specific phone numbers, or email addresses aren't blocked.

Even though you don't receive blocked messages on your smartphone, blocked messages might contribute to data usage in your wireless service plan. You can stop email messages from being forwarded to your smartphone by turning off email message forwarding or by using email message filters.

Cleaning memory

By default, your BlackBerry smartphone continually cleans temporary memory to remove sensitive data that is no longer being used.

Your smartphone can perform the following additional cleaning actions:

- overwrite memory

- periodically run the memory cleaning application, which causes applications to empty any caches, free memory, and automatically overwrite the freed memory

Your smartphone performs additional cleaning actions during any of the following situations:

- you turn on encryption
- a third-party application that you have downloaded registers with the memory cleaning application

You can set the memory cleaning application to run when you insert your smartphone into the holster or when your smartphone remains idle for a specified period of time. You can also manually run the memory cleaning application on your smartphone, and turn on or turn off memory cleaning.

Deleting all BlackBerry smartphone data

Your BlackBerry smartphone is designed to permanently delete your data when you wipe your smartphone or type your smartphone password incorrectly more than 10 times. When you wipe your smartphone, you can also set your smartphone to remove all third-party applications and application data from your smartphone.

If you resell your smartphone, remember to delete all of your data so that the person that buys your smartphone can't access your personal information.

For more information about preparing your smartphone for resale, visit www.blackberry.com/btsc to read article KB05099.

Find more information

- Find step-by-step instructions in the user guide for your BlackBerry smartphone. Click Help on the home screen or in an application menu. Or visit www.blackberry.com/docs/smartphones.
- For information about security features for other BlackBerry products, visit www.blackberry.com/security.

Legal notice

©2012 Research In Motion Limited. All rights reserved. BlackBerry®, RIM®, Research In Motion®, and related trademarks, names, and logos are the property of Research In Motion Limited and are registered and/or used in the U.S. and countries around the world.

Bluetooth is a trademark of Bluetooth SIG. Wi-Fi is a trademark of the Wi-Fi Alliance. All other trademarks are the property of their respective owners.

This documentation including all documentation incorporated by reference herein such as documentation provided or made available at www.blackberry.com/go/docs is provided or made accessible "AS IS" and "AS AVAILABLE" and without condition, endorsement, guarantee, representation, or warranty of any kind by Research In Motion Limited and its affiliated companies ("RIM") and RIM assumes no responsibility for any typographical, technical, or other inaccuracies, errors, or omissions in this documentation. In order to protect RIM proprietary and confidential information and/or trade secrets, this documentation may describe some aspects of RIM technology in generalized terms. RIM reserves the right to periodically change information that is contained in this documentation; however, RIM makes no commitment to provide any such changes, updates, enhancements, or other additions to this documentation to you in a timely manner or at all.

This documentation might contain references to third-party sources of information, hardware or software, products or services including components and content such as content protected by copyright and/or third-party websites (collectively the "Third Party Products and Services"). RIM does not control, and is not responsible for, any Third Party Products and Services including, without limitation the content, accuracy, copyright compliance, compatibility, performance, trustworthiness, legality, decency, links, or any other aspect of Third Party Products and Services. The inclusion of a reference to Third Party Products and Services in this documentation does not imply endorsement by RIM of the Third Party Products and Services or the third party in any way.

EXCEPT TO THE EXTENT SPECIFICALLY PROHIBITED BY APPLICABLE LAW IN YOUR JURISDICTION, ALL CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS, OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY CONDITIONS, ENDORSEMENTS, GUARANTEES, REPRESENTATIONS OR WARRANTIES OF DURABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, MERCHANTABILITY, MERCHANTABLE QUALITY, NON-INFRINGEMENT, SATISFACTORY QUALITY, OR TITLE, OR ARISING FROM A STATUTE OR CUSTOM OR A COURSE OF DEALING OR USAGE OF TRADE, OR RELATED TO THE DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN, ARE HEREBY EXCLUDED. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY BY STATE OR PROVINCE. SOME JURISDICTIONS MAY NOT ALLOW THE EXCLUSION OR LIMITATION OF IMPLIED WARRANTIES AND CONDITIONS. TO THE EXTENT PERMITTED BY LAW, ANY IMPLIED WARRANTIES OR CONDITIONS RELATING TO THE DOCUMENTATION TO THE EXTENT THEY CANNOT BE EXCLUDED AS SET OUT ABOVE, BUT CAN BE LIMITED, ARE HEREBY LIMITED TO NINETY (90) DAYS FROM THE DATE YOU FIRST ACQUIRED THE DOCUMENTATION OR THE ITEM THAT IS THE SUBJECT OF THE CLAIM.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, IN NO EVENT SHALL RIM BE LIABLE FOR ANY TYPE OF DAMAGES RELATED TO THIS DOCUMENTATION OR ITS USE, OR PERFORMANCE OR NON-PERFORMANCE OF ANY SOFTWARE, HARDWARE, SERVICE, OR ANY THIRD PARTY PRODUCTS AND SERVICES REFERENCED HEREIN INCLUDING WITHOUT LIMITATION ANY OF THE FOLLOWING DAMAGES: DIRECT, CONSEQUENTIAL, EXEMPLARY, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR AGGRAVATED DAMAGES, DAMAGES FOR LOSS OF PROFITS OR REVENUES, FAILURE TO REALIZE ANY EXPECTED SAVINGS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, LOSS OF BUSINESS OPPORTUNITY, OR CORRUPTION OR LOSS OF DATA,

FAILURES TO TRANSMIT OR RECEIVE ANY DATA, PROBLEMS ASSOCIATED WITH ANY APPLICATIONS USED IN CONJUNCTION WITH RIM PRODUCTS OR SERVICES, DOWNTIME COSTS, LOSS OF THE USE OF RIM PRODUCTS OR SERVICES OR ANY PORTION THEREOF OR OF ANY AIRTIME SERVICES, COST OF SUBSTITUTE GOODS, COSTS OF COVER, FACILITIES OR SERVICES, COST OF CAPITAL, OR OTHER SIMILAR PECUNIARY LOSSES, WHETHER OR NOT SUCH DAMAGES WERE FORESEEN OR UNFORESEEN, AND EVEN IF RIM HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW IN YOUR JURISDICTION, RIM SHALL HAVE NO OTHER OBLIGATION, DUTY, OR LIABILITY WHATSOEVER IN CONTRACT, TORT, OR OTHERWISE TO YOU INCLUDING ANY LIABILITY FOR NEGLIGENCE OR STRICT LIABILITY.

THE LIMITATIONS, EXCLUSIONS, AND DISCLAIMERS HEREIN SHALL APPLY: (A) IRRESPECTIVE OF THE NATURE OF THE CAUSE OF ACTION, DEMAND, OR ACTION BY YOU INCLUDING BUT NOT LIMITED TO BREACH OF CONTRACT, NEGLIGENCE, TORT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND SHALL SURVIVE A FUNDAMENTAL BREACH OR BREACHES OR THE FAILURE OF THE ESSENTIAL PURPOSE OF THIS AGREEMENT OR OF ANY REMEDY CONTAINED HEREIN; AND (B) TO RIM AND ITS AFFILIATED COMPANIES, THEIR SUCCESSORS, ASSIGNS, AGENTS, SUPPLIERS (INCLUDING AIRTIME SERVICE PROVIDERS), AUTHORIZED RIM DISTRIBUTORS (ALSO INCLUDING AIRTIME SERVICE PROVIDERS) AND THEIR RESPECTIVE DIRECTORS, EMPLOYEES, AND INDEPENDENT CONTRACTORS.

IN ADDITION TO THE LIMITATIONS AND EXCLUSIONS SET OUT ABOVE, IN NO EVENT SHALL ANY DIRECTOR, EMPLOYEE, AGENT, DISTRIBUTOR, SUPPLIER, INDEPENDENT CONTRACTOR OF RIM OR ANY AFFILIATES OF RIM HAVE ANY LIABILITY ARISING FROM OR RELATED TO THE DOCUMENTATION.

Prior to subscribing for, installing, or using any Third Party Products and Services, it is your responsibility to ensure that your airtime service provider has agreed to support all of their features. Some airtime service providers might not offer Internet browsing functionality with a subscription to the BlackBerry® Internet Service. Check with your service provider for availability, roaming arrangements, service plans and features. Installation or use of Third Party Products and Services with RIM's products and services may require one or more patent, trademark, copyright, or other licenses in order to avoid infringement or violation of third party rights. You are solely responsible for determining whether to use Third Party Products and Services and if any third party licenses are required to do so. If required you are responsible for acquiring them. You should not install or use Third Party Products and Services until all necessary licenses have been acquired. Any Third Party Products and Services that are provided with RIM's products and services are provided as a convenience to you and are provided "AS IS" with no express or implied conditions, endorsements, guarantees, representations, or warranties of any kind by RIM and RIM assumes no liability whatsoever, in relation thereto. Your use of Third Party Products and Services shall be governed by and subject to you agreeing to the terms of separate licenses and other agreements applicable thereto with third parties, except to the extent expressly covered by a license or other agreement with RIM.

Certain features outlined in this documentation require a minimum version of BlackBerry Enterprise Server, BlackBerry Desktop Software, and/or BlackBerry Device Software.

The terms of use of any RIM product or service are set out in a separate license or other agreement with RIM applicable thereto. NOTHING IN THIS DOCUMENTATION IS INTENDED TO SUPERSEDE ANY EXPRESS WRITTEN AGREEMENTS OR WARRANTIES PROVIDED BY RIM FOR PORTIONS OF ANY RIM PRODUCT OR SERVICE OTHER THAN THIS DOCUMENTATION.

Research In Motion Limited
295 Phillip Street

Waterloo, ON N2L 3W8
Canada

Research In Motion UK Limited
200 Bath Road
Slough, Berkshire SL1 3XE
United Kingdom

Published in Canada